zSeries災害対策サービスの紹介
Introduction of zSeries Disaster Recovery Service

藤井　欽文　　中島　卓
Tadafumi Fujii　Taku Nakajima

概要

ITを活用した競争社会では、情報の連携度を高めることで競争優位性を得るビジネスアプリケーション（SCM、CRM、SFAなど）がITインフラ上で多数稼動している。この状況下において一企業に起きた災害の影響範囲は、その企業にとどまらず、取引企業や業界をも巻き込んだ経済社会へと広がっている。結果として災害に対する想定被害額も増加しており、災害対策への関心が高まってきている。

本稿ではITインフラに対する災害対策の方法論を整理し、当社で取り組んでいるzSeries災害対策サービスについて述べる。第1章では企業の事業継続（Business Continuity）の必要性について、第2章では災害対策のレベルに応じた災害対策の手法と方法論について述べる。第3章ではzSeries災害対策サービスの特徴であるデータ遠隔コピーの技術、自動化運用、および災害に強いデータセンターの特徴と利点について述べる。第4章と第5章では、GDPS/XRCとPPRC-XDの2つのサービスを技術的な観点で説明する。

1. 災害対策の必要性

まず、「災害」を辞書で引くと、「地震・台風・洪水・津波・噴火・旱魃（かんばつ）・大火災・伝染病などによって引き起こされる不時のわざわい。また、それによる被害。」(1) とある。これら自然による災害（広域）以外の人的災害（局所：テロ、立てこもり、放火事件、ヘリコプター墜落事故など）なども合わせた災害は、世界中で毎日の様にどこかで発生している。万が一災害でデータセンターが壊滅的な打撃を受けた場合、ゼロからの復旧は数週間から数ヵ月以上かかると予想される。企業のシステム部門を対象とした調査によれば基幹システムが停止した場合1日あたりの想定被害額は52.7%の企業が1千万円以上、さらに10.7%の企業が10億円以上と回答している(2)。このようにITインフラを生命線としている現在の企業において災害対策の有無は事業継続に大きな影響を及ぼし、企業存続に関わる重大なテーマである。

2. 災害対策の方法論

2.1 災害対策のポイント

災害対策では本番サイトが使用できなくなったときの事業継続を目的としている。このことから、一般的に以下の3点が災害対策のポイントとなる。

- 地理的に分散した場所にバックアップ用設備を準備すること
- データをできるだけ完全な形で復元（バックアップとリストアの完全性）すること
- 業務サービスを再開するためできるだけ早くシステムを構築（復旧）すること

これらのポイントを完全に満たす事が理想的な災害対策ではあるが、トレードオフとしてコストは上昇する傾向にある。従って、次節以降に述べる検討要素をもとにコストバランスを考慮しながら対策を講じる必要がある。

2.2 災害対策の計画

災害対策策定において、まず次のような検討要素をもとに対策の方針を決定する。

- 災害対策の対象業務システム選定及び優先付け
- RTO（Recovery Time Objective）：復旧目標時間
  システム停止の許容時間
- RPO（Recovery Point Objective）：復旧目標ポイント
  データロスの許容範囲

表1　災害対策のレベルと手法

Level	手　　法	RPO	RTO
レベル0 No off-site Data	災害対策用の遠隔地保管データは存在しない。	NA	NA
レベル1 Data backup with no Hot-site	遠隔地にデータを保管。一般的にはテープにデータを入れてPTAMで陸送。PTAM（Pickup Truck Access Method）：トラックによる陸送	1日-1週間	数週間-数ヵ月
レベル2 Data backup with a Hot-site	PTAMに加え、復旧用のサイトを保持している。	1日-1週間	24-72時間
レベル3 Electronic Vaulting	レベル2に加え、一部重要なデータは伝送。その他のデータはPTAMで陸送。	24時間以内	24時間以内
レベル4 Point-in-time Copies	Batch/Online DBのShadowing&Journaling，PointIn Timeコピーの繰り返し。ファジーコピーの非同期ディスク・ミラーリング。	0.5−12時間	12時間以内
レベル5 Transaction Integrity	本番システムと復旧用システムを持つ。ソフトウェアによるデータ二重化。2フェーズコミット。	1分以内	1-8時間
レベル6 Zero or little data Loss (Remote Disk Mirroring)	遠隔地システムとローカル・システムでDISKミラーリング。被災時は遠隔地システムで再立上げ	0-数秒	1-4時間
レベル7 Highly automated, Business integrated solution	レベル6に自動化機能を統合。手動よりもより迅速で信頼性の高い復旧。	0-数秒	数十秒-1時間

コスト大

災害対策レベル*:1992年米国Share User GroupとIBM社で定義したレベルをベースに最新の技術とRPO/RTOを反映したレベルに更新

●バックアップ施設の要件（地理的位置、建物構造、電源設備、セキュリティ設備等）

設定したRTO、RPOに対する災害対策の手法を具体化させ、さらに詳細な設計及び事業継続計画（Business Continuity Plan）を作成する。RTO、RPOはゼロに近づくほど連続稼動性が高くなり高度な災害対策となる。しかし、同時にコスト上昇にも繋がるため、災害損失額と対策費用のバランスを考慮しながら最適な目標を設定することが重要である。表1は災害対策レベルと対策手法を分類したものである。

2.3 災害対策の管理手法

事業継続計画では守るべき情報資産を分類・把握し、全体最適を見据えてシステムの災害対策を策定する。その管理手法として、情報セキュリティマネージメントシステム（ISMS）の管理手法のフレームワークが有効である。ISMSは、社内の全ての情報資産を機密性・完全性・可用性により分類・重み付けし、情報セキュリティ対策を検討し、PDCAの継続した管理サイクルで運用される（表2参照）。特に定期的な災害リハーサルをC（チェックフェーズ）で実施することで、2.1節で説明した「災害対策のポイント」の実効性を運用評価することができる。

表2　事業継続計画

計画PDCA（案）　　事業継続計画（サンプル）

期　間	項　目	実　施　内　容
災害対策の具体的計画 Plan	範囲の決定 情報の洗い出し リスクの評価 管理目的の決定	どの業務システム（まもるべき情報資産の決定） どの情報（帳票類、マスター、プログラムetc） 機密性、完全性、可用性 RPO、RTO、適用可能な保険の検討、損失額の決定、 戦略計画（長・中・短）の承認
計画の実装・実施・運用 Do	リスク対応計画のまとめ リスク対応計画の実施 管理策の実施	具体策の計画、定期的なリハーサル（テスト）方法、 リカバリ手順とシステム更新方法の明文化 対策実装 導入時の想定評価レベル、運用上の不具合を関係者で認識
実施の結果検証（監査） Check	監視手順の実施 定期レビューの実施 リスクレベルのレビュー	実装習熟度ヒアリング、評価 リハーサル（テスト）の実施、評価 情報セキュリティー一覧表作成
経営観点からの改善・見直し Act	改善項目の実施 予防処置の実施 運用上の問題解決 管理目的の達成確認	次管理策の検討 現行管理策の問題解決 運用上の不具合 RPO、RTO、損失額の決定、コストの算定、開始時期の確認、リスク対策の評価、IT戦略計画の評価

3. zSeries災害対策サービス概要

当社は日本IBM株式会社（以下、IBM社）、株式会社アット東京(以下、アット東京社)と3社協業によりeServer zSeries（以下、zSeries）を対象とした災害対策サービスを提供している。このサービスは単なるデータ遠隔ミラーリングだけではなく、バックアップマシンと運用監視、さらにバックアップ施設を含めた総合的なソリューションである。

3.1 サービスの特徴

zSeries災害対策サービスの特徴は以下のとおりである。

●IBM社製zSeriesシステムを対象としたサービス

●RTO/RPOを極小化する先進のディスク遠隔コピー技術
●GDPSによる災害対策向け自動化運用（詳細は3.3参照）
●最高レベルの堅牢さと設備を持つバックアップサイト
●短期間で災害対策環境を構築可能なシンプル構成

このように前章で述べた災害対策のポイントに加え、自動運用や堅牢なバックアップ施設を含めた総合的な災害対策環境を低コストで構築、運用することが可能となる。

3.2 データ遠隔コピー技術

ディスクのデータ遠隔コピー方法をコピーするタイミングで分類すると次のように分けられる。

●同期コピー
プライマリデータとセカンダリデータが常に同一な状態に保たれるためデータロスは発生しない。しかし同時に両方のディスクへI/O処理が発生するためパフォーマンスに影響を及ぼす可能性がある。従ってサイト間が近距離であることや高速ネットワークが設計条件となる。

●非同期コピー
セカンダリデータのI/O処理は非同期で行われるため、本番システムのパフォーマンスへの影響は軽微であり距離やネットワークの条件も同期コピーに比べ緩和される。ただしプライマリデータとセカンダリデータが同一ではないためデータの整合性を保つ仕組みが必要となる。

また、データコピーの実装方法で分類すると次のように分けられる。

●ソフトウェア実装型
運用ツールやアプリケーションとの連携が容易となるが、パフォーマンスへの影響や取り扱えるデータの種類が限定されるなど制約が多い。

●ハードウェア実装型
データの種類やアプリケーションに依存しないが、一般的に運用ツールなどとの連携が困難である。

●ハードウェア・ソフトウェア混成実装型
上記2つの実装型の欠点を補い、運用ツールなどの連携とデータの種類やアプリケーションに依存しないデータコピーを実現する。

zSeries災害対策サービスでは同期･非同期コピーとも対応可能であり、データやアプリケーションに依存しないハードウェア･ソフトウェア混成実装型である。そのため、システム規模や復旧要件、予算枠によって柔軟且つ最適な構成が選択可能となる。

3.3 GDPSの自動化運用

GDPS（Geographically Dispersed Parallel Sysplex）とは災害対策システムを統合的に運用管理するIBM社の自動化ソリューションである。従来人手を要したコピー監視制御やシステム切り替えなどの運用を自動化し僅かな負荷で確実に実施することが可能である。主な機能は以下のとおりである。

●簡易パネルによる監視制御が可能（特殊なコマンドは不要）
●複数ディスク間のコピー監視制御
●データ整合性維持管理
●スクリプトによる自動オペレーション（バックアップシステムへの切り替えなど）

3.4 最高レベルのバックアップ施設

当サービスはバックアップ施設として世界最高レベルの堅牢な設備を持つアット東京社データセンターを活用する。従来は災害を共有しないようにサイト間の距離が重要視され、遠距離に分散する形態が一般的であったが、災害時に影響がないほど堅牢なバックアップ施設であればサイト間の距離は特に重要ではない。アット東京社データセンターは地震リスク分析において世界規模のリスクマネジメント会社より最高ランク（PML値(*1)最小）を取得しており建物の堅牢さだけではなくセキュリティ、電源供給、ネットワーク設備など全てにおいて最高レベルのスペックを備えたバックアップ施設である。

4. GDPS/XRCサービス

zSeries災害対策サービスは幾つかの提供タイプがあり、システム規模や要件により選択できる。本章では設計条件の柔軟さやコストバランスの面から現在の主力サービスであるGDPS/XRCサービスとPPRC-XDサービスについて説明する。

4.1 概説

GDPS/XRCサービスにはGDPSの運用監視機能とIBM社製Enterprise Storage Serverディスク装置（以下ESS）のXRC（eXtended Remote Copy）と呼ばれるコピー技術を組み合わせた高度な災害対策サービスである。ハードウェア・ソフトウェア混成実装型の非同期コピーをベースとし、次の特徴がある。

●RTOは数分から数十分以内、RPOは数秒程度を実現(レベル7)。
●ディスク間はXRCによる非同期コピー、GDPSによるデー

(*1) PML（Probable Maximum Loss）：再現期間500年の大地震による予想最大損失率であり、建物の地震リスク評価に用いられる。

タ整合性を確保。

- データの種類やアプリケーションに依存しない全量コピー方式。
- 本番システムのパフォーマンスに影響が軽微。
- 高速ネットワークは必須ではなく、サイト間の距離制限もない。
- バックアップ用マシンのz/OS（もしくはOS/390）でXRCの運用監視や操作を実施。

4.2 XRCの仕組み

図1にGDPS/XRCの基本的なシステム構成を示す。バックアップマシン側z/OSの標準コンポーネントであるSDM（System Data Mover）がデータの整合性を制御する。このため、本番システムのパフォーマンスに影響が少ない。また、バックアップシステム構築時に本番システムへの変更も殆ど必要ない。

①プライマリシステムからプライマリESSへデータ更新処理更新データにWRITEのタイムスタンプ情報を付加してESSのキャッシュ上に保管。

②プライマリESSより更新処理完了を通知しプライマリシステム処理は完了。

③セカンダリzSeriesのSDMがプライマリESSのキャッシュから更新データを読み取る。

④SDMが更新データのタイプスタンプ情報をもとに正しい更新順序と同期点を持つデータのグループを作成。

⑤SDMからジャーナルデータセットに④のグループを書き出し。

⑥SDMがジャーナルデータセットをもとにセカンダリESSにグループを書き出す。

⑦グループがセカンダリESSに書き出された事をコントロールデータセットに記録。

4.3 GDPS/XRCのシステムデザインと構成要素

（1）本番サイト

- プライマリシステム（本番システム）
- プライマリESS（XRC機能が必須、キャッシュサイズは16GB以上が推奨）
- プライマリデータ（XRCのコピー元データ）

（2）バックアップサイト

- セカンダリシステム（通常は非稼動）
- セカンダリESS（XRC機能は不要）
- セカンダリデータ（XRCのコピー先データ）
- Tertiaryデータ

  セカンダリデータをFlashCopy（*2）にてバックアップしたデータ。必須ではないが準備することで以下のメリットがある。

  ア）運用中（XRC設定変更や障害対応時の初期コピー中）に被災した場合でも整合性のあるTertiaryデータが確保される。

  イ）システムの切り替えリハーサルにTertiaryデータを使用することでXRCコピー中断やセカンダリデータの更新が避けられる。

- SDMシステム（XRCにおけるコピー管理・実施を行うSDMが稼動するシステム）
- Kシステム（SDMシステムと連携しXRCの状況監視・操作を行うシステム）
- GDPS（SDMとKシステムでz/OSのNetviewのアプリケーションとして稼動。GDPS監視端末によりコピー監視や操作を簡易的に行うことが可能）

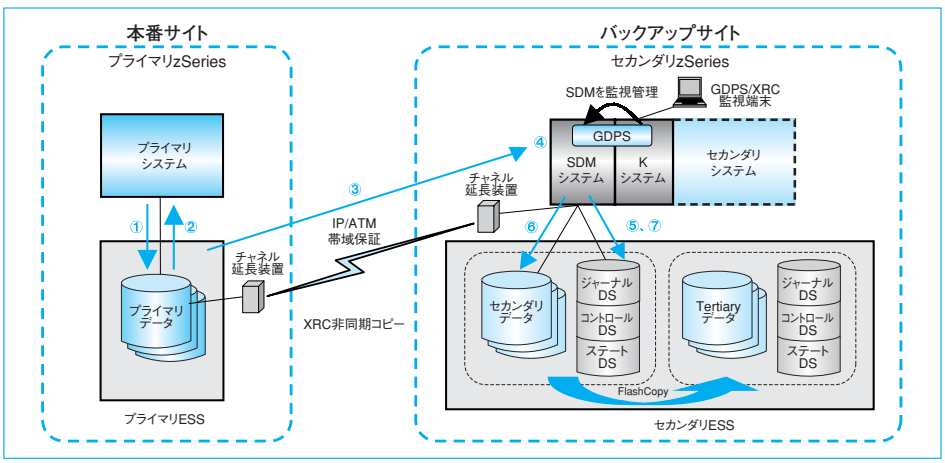

図1　GDPS/XRCシステム構成図

（*2）FlashCopy：ESS内でバックアップデータを瞬時に取得する機能。バックグラウンドでデータコピーや参照更新制御が行われる。

●サイト間ネットワーク（ESCONもしくはFICON接続となりチャネル延長装置経由でIP/ATMネットワーク接続）

このように通常時はSDMシステムとプライマリESSがネットワーク経由で接続され、データの整合性を保ちながら非同期コピーを行う。そして被災時には整合性の取れたTertiaryデータ（もしくはセカンダリデータ）を用いてセカンダリシステムを起動する流れとなる。

4.4 運用のシナリオ

運用監視及び操作は全てGDPS監視端末より行う。システム環境や要件にもよるが、ここでは標準的な運用のシナリオを説明する。

（1） 初期コピー運用（初回や構成変更時、障害復旧後の全データコピー。環境セットアップが完了している事が前提）

①GDPS監視端末よりXRCのコピー開始で初期コピー実施

②初期コピーが完了後一時停止し、FlashCopyによりセカンダリデータをバックアップ（Tertiaryデータの保管）

③XRCを再開・再コピー → 非同期モードによるコピー開始

④業務処理開始

（2） 通常運用（通常のXRCコピー状況の監視、一時停止や再開操作）

①GDPS監視端末より以下の項目を定期的に監視

●全コピーのステータス、ボリューム数監視

●DELAY値（プライマリデータとの時間差）チェック（通常数秒から数分程度）

②システム障害や保守時、業務要件によるXRCの一時停止再開

（3） 被災時システム切り替え運用（被災時セカンダリシステムへの切り替え操作）

①GDPS監視端末より予め作成済のシステムの切り替え用スクリプトを起動（スクリプトにより以降の処理が全て自動実行）

②XRCを停止し、FlashCopyにてセカンダリデータをTertiaryデータへバックアップ

③Tertiaryデータに対しジャーナルデータセットの未反映データを更新

④Tertiaryデータのディスクボリューム名を本番ボリュームと同名にリネーム

⑤Tertiaryデータを使用しセカンダリシステムの起動（主要タスクまでの起動）

⑥業務サービス再開は状況により手動操作（スクリプトによる自動起動も可能）

このようにGDPS監視端末から全ての監視や操作が可能であり、特に被災時の混乱した状況においてもスクリプトの実行だけで迅速且つ確実にシステムを切り替える事ができる。アット東京社のGDPS/XRCデモシステムではシステムの切り替えの所要時間は3分程度である。実際の大規模な環境においても10分以内に切り替えることが可能である。

5. PPRC-XDサービス

5.1 概説

PPRC（Peer-Peer Remote Copy）- XDサービスはGDPSによる運用監視機能はなくGDPS/XRCに比べ構築の負荷やコストを抑えた簡易版サービスである。当サービスはESSハードウェア実装型の非同期コピー技術を使用したソリューションであり、次のような特徴がある。

●RTOは数時間以内、RPOは数時間～1日を実現（レベル4）。

●ディスク間は非同期コピーでセカンダリデータの整合性はない。整合性を保つために定期的な同期点の取得操作が必要。

●ESSのハードウェア機能によるコピーのため、OSなどソフトウェアは不要。

●データの種類やアプリケーションに依存しない全量コピー方式。

●本番システムのパフォーマンスに影響が軽微。

●高速ネットワークは必須ではなく、サイト間の距離制限もない。

●GDPSは未対応であり運用監視・操作を自動化する場合本番システム側で別途運用環境の構築が必要。

5.2 PPRC-XDの仕組み

ESS間のコピー技術には前述のXRCとハードウェア機能によるPPRCがある。PPRCはもともと同期コピーであったが、非同期コピーとしてPPRC-XD（Extended Distance）が追加された。図2にPPRC-XDのコピー機能をベースにバックアッ

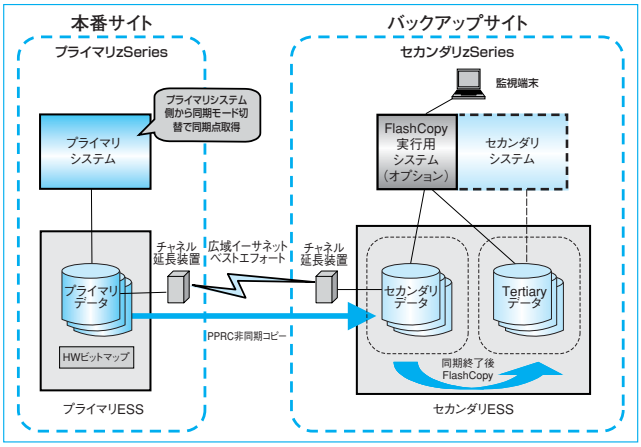

図2　PPRC-XDシステム構成図

プマシンを組み合わせたシステム構成を示す。

①プライマリESS内のキャッシュ上にハードウェアビットマップ（以下HBM）が生成

②データ更新処理時にHBMに更新ビットが立つ→データ更新処理は終了

③ESSがHBMをサーチし、更新ビットのあるデータをセカンダリESSへ転送し更新

このように非同期でコピーされるため本番処理への影響はないが、更新順序を考慮していないためセカンダリデータの整合性は保証されない。そこで定期的に同期点を取得し整合性のあるセカンダリデータをバックアップし被災時はそのデータを使用する。

5.3 PPRC-XDサービスの運用シナリオ

PPRC-XDの監視や同期点の取得は全てプライマリシステム側で実施するが、GDPS未対応のため手動もしくはNetviewなどの自動監視ツールを活用する必要がある。

PPRC-XDの通常運用とシステム切り替えの流れを以下に述べる。

（1）通常運用

①プライマリシステムよりPPRC-XDのコピー状況監視

②業務処理の終了タイミングで同期モードへの変更コマンドを投入し同期点取得

③PPRC-XDを一時停止させ、FlashCopyによりセカンダリデータをバックアップ（Tertiaryデータの保管）

④PPRC-XDの再開コマンド投入し、業務処理再開

（2）被災時システム切り替え運用

Tertiaryデータを使用し運用手順に従いバックアップシステム起動（セカンダリデータは整合性が無いため使用不可）

この運用の重要なポイントは同期点取得にあり、取得する頻度によりRPOが左右される。1日1回の同期点取得であれば最大1日分のデータロスとなり、取得する頻度が多ければその分データロスが減少する。本番業務に影響を及ぼさない程度に同期点を多く取得する事が重要なポイントである。

6. おわりに

災害対策は保険と同様にそれ自体は利益を生むものではない。しかし、企業活動の根幹となったITインフラの事業継続計画は企業の存続にかかわる重要なテーマであり、株主や社会に対する企業責任となってきている。本稿で説明したGDPS/XRCやPPRC-XDサービスは、遠隔2サイト間の全量コピー、低負荷で安定した運用などの高度なシステム災害対策としての優位性がある。しかし、システム以外の要素（事務所、従業員など）を含めて継続的な事業継続計画の見直しが必要不可欠であると認識すべきである。私たちは、今後IBM社やアット東京社と協力しながら課題をクリアし、より低コストで実効性がある災害対策ソリューションを提供していきたい。

参考文献

（1）三省堂：大辞林 第二版

（2）日本情報処理開発協会：平成15年度情報セキュリティに関する調査 集計結果p.5,（2002）

（3）アット東京社Webサイト,http://www.attokyo.co.jp/

（4）IBM Red Book（February 2004）The Total Storage Solutions Handbook

藤井　欽文
Tadafumi Fujii

・アウトソーシング事業本部
サービス事業推進部
・アウトソーシングサービスの受注支援業務を担当

中島　卓
Taku Nakajima

・アウトソーシング事業本部
アウトソーシング・サービス・センター
・システム運用管理を中心としたアウトソーシング業務に従事